

AU/ACSC/DILLARD/AY10

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

A CYBER SPECIAL PROGRAM OFFICE: MANAGING THE ENTERPRISE AS A
WEAPON SYSTEM FOR BETTER INFORMATION SHARING IN THE DOD

By

Wade E. Dillard, Major, U.S. Air Force

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Mr. Roger Philipsek, DAF

Maxwell Air Force Base, Alabama

April 2010

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government. This document is only releasable through government permission; see the attached Standard Form 298 for details.



Table of Contents

ACKNOWLEDGEMENTS	4
ABOUT THE AUTHOR	5
EXECUTIVE SUMMARY	6
BACKGROUND	6
Introduction	6
Air Force Technology History	7
Technology Evolution in Air Force History	8
Cyberspace and Air Force History	8
DEFINING THE CHALLENGES	9
Introduction	9
Research Scope	9
Research Questions	10
Defense Science Board Task Force Findings	10
Metadata Explained	12
Metadata Example	12
Air Force Metadata Example	12
Complex Metadata Example	13
Cyberspace Manning	13
SOLVING CHALLENGES	14
Cyber SPO Creation	14
SPO Justification and Roles	15
SPO Benefits	15
Current Challenges	16
Cyber Operation Comparison	16
IMPLEMENTATION	17
Introduction	18
Initial Macro Level Issues	18
Initial Intermediate Level Issues	21
Initial Micro Level Issues	22
SPO Structure Recommendation	23
Cyber SPO Feasibility and Alternatives	25
Continuing Research Areas	26
Air Force Example Revisited	27
CYBER SPO IMPACT ON DOD 8320.02	28
CONCLUSION	29
ENDNOTES	30
BIBLIOGRAPHY	31
APPENDIX A - CYBER REQUIREMENT CHECK LIST TEMPLATE	32
APPENDIX B - REQUIREMENTS STRENGTH INDICATOR PROCESS	39

ACKNOWLEDGEMENTS

My thanks to Mr. Shea, Office of the Secretary of Defense, Chief Information Officer for allowing my investigation on this important topic. In addition, my appreciation to Mr. Roger Philipsek, ACSC faculty, his support allowed the latitude necessary for researching such a broad subject area. My special thanks to my grandfather, Wallace E. Dillard, whose Army Air Corps experiences and stories led me to military service. Thank you to my wife and our children, I appreciate your understanding while researching and writing this paper. Time is the one commodity we never get again and family time is the most precious—thank you for sharing your time with the United States Air Force.



ABOUT THE AUTHOR

Major Wade Dillard (BSCS, Park University, MSCE, Air Force Institute of Technology, MBA, and St Mary's University) enlisted in the Air Force in 1990 and spent eight years, across three assignments, in electronic aircraft maintenance as a test measurement and diagnostic technician. In this field, he calibrated and repaired aircraft instrumentation, airfield navigation equipment, and a wide variety of communications assets. Upon completing his degree, he received a commission from Officer Training School (OTS), Maxwell Air Force Base (AFB) in 1998. After OTS, he attended the Air Force's basic communications course at Keesler AFB, and entered the communications and information career field. His first assignment, RAF Croughton, UK, from 1999 to 2001, he served as commander for the installation's Systems Flight providing communications to Operation Allied Force in Kosovo. Returning to the United States, he attended the Air Force Institute of Technology (AFIT) at Wright-Patterson AFB researching wireless system solutions for the Air Force Research Laboratory. In 2003, Major Dillard departed AFIT for Headquarters, Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA) at Lackland AFB, Texas. There he served as a program manager for AFISRA's global networks, in strategic plans, and as an executive officer. In 2007, he left Texas to lead 135 Airmen as an airborne communications officer, managing nuclear command and control systems on the E-4B "flying Pentagon" at Offutt AFB, Nebraska. In 2009, after flying 86 missions on the E4-B and OC-135, he was selected to attend Air Command and Staff College at Maxwell AFB. Major Dillard has earned three Meritorious Service Medals, an Air Medal, as well as several Air Force Commendation and Achievement Medals. He has been married for 24 years and has three children.

Digital Collections
Air University—Maxwell AFB, AL

EXECUTIVE SUMMARY

Department of Defense (DOD) standard 8320.02 establishes the need for all subordinate organizations to share information through metadata tagging of information. The United States Air Force's recent consolidation of cyber capabilities under the 24th Numbered Air Force formerly AFCYBER, under the Air Force Space Command (AFSPC) major command, and the DOD's proposed United States Cyber Command (USCYBERCOM) arrange the strategic levels of cyber capabilities. However, to meet DOD Standard 8320.02 on the operational and tactical levels, Air Force leaders need to establish a special program office (SPO), or cyber SPO, which collectively manages all cyber and communications assets providing standardized, integrated systems, with consolidated, cradle-to-grave asset and information management similar to existing aircraft and space platform SPOs. This research paper conceptually envisions a proposed framework for how a cyber SPO would look, function, and its initial focus items and its efforts to meet DOD Standard 8320.02, for information sharing. Using the proposed cyber SPO solutions and resulting efforts to meet the 8320.02 standard, the Air Force has the opportunity to save a minimum of 21.8 million dollars per year in network costs, thousands of man hours in reduced information processing times, and improving workflow processes across the Air Force. Applied across the DOD's total population, there is a potential opportunity, for saving an additional 128 million dollars (approximate) in network costs utilizing the same cyber SPO concepts, with even greater work force, man hour savings.

BACKGROUND

Introduction

Most Air Force communications and cyber management functions, programs, planning, funding, and acquisition processes currently exist in many forms, albeit separated from each

other by organizational boundaries. Therefore, the U.S Air Force should seek to merge its cyber and communications platforms management and information technologies the same way it has with other “weapon” platforms by creating a formal, consolidated special program office for all communications, cyber, and IT systems. This integration is the next logical step following the creation of the AFCYBER and USCYBERCOM. By building a cyber SPO, the Air Force, and through time the other Department of Defense (DOD) services, can centrally govern the Information Technology (IT) systems and information; thus reaching the overarching goals of DOD standard 8320.02 more effectively, efficiently, and earlier than current ad-hoc methods allow. This research paper does not narrowly focus on the technology of DOD Standard 8320.02 as much as it is proposes a SPO construct to build the organization for pulling technology efforts and existing entities together to meet the standard’s intent.

Air Force Technology History

In the book, *Strategic Warfare in Cyberspace*, Dr Rattray relates how leadership, prior to the Second World War, focused solely on the bomber community to the neglect of pursuit and fighter escorts almost to the detriment of losing the war. He rightly contends this bomber-centric focus is similar to the underdeveloped strategic vision the cyber community faced in its early days and the importance of peacetime development of doctrine and wartime learning.¹ Cyber capabilities, much like early WWII fighter escort requirements, have emerged as a strategic pivot point for the Air Force, fellow services, and the Department of Defense to require its own organizations. The new joint cyber command and related 24th Numbered Air Force have given a new home and broad mission context to former support functions, which are now operational in nature. These organizations are equally as pivotal and evolutionary as the initial creation of the Army Air Forces.

Technology Evolution in Air Force History

This first evolution of formalizing cyber resources requires the Air Force to once again look into its past to avoid making the same evolutionary missteps it made as new capabilities appeared. Not only did leaders struggle with the previously mentioned fighter evolution, but it also struggled with strategic bombing concepts with the arrival of the intercontinental ballistic missile (ICBM).² Ultimately, the Air Force's bomber and ICBM doctrinal ambiguity led, ironically, to the dominance of fighter aircraft community, at least until the recent arrival of remotely piloted vehicles and the revolution in information technology and global communications. The challenges faced in the cyber community are now similar to General William Tunner's challenges from the early airlift days. General Tunner's challenge, in World War Two, was to modernize airlift while the technology was evolving as well as in high demand. This is exactly, the challenge the cyber community faces in the modern era.³

Cyberspace and Air Force History

How do modern cyber issues relate to early airlift? They share virtually the same traits. First, both are expected to be available 24/7 and able to deliver their products under adverse conditions. As, Services have become reliable the greater the magnitude of demands are placed on the platforms. Much like air supremacy and airlift, United States forces consistently seem to assume cyber-based services are available, reliable, attributable, and operate with no interruption. Second, early airlift and modern cyber platforms were not "standardized" across all commands, thus they required a wider range of services and funds to keep operational. General Tunner, had to contend with over 150 aircraft platforms, similar to the way modern IT systems have hundreds of varieties of hardware and software combinations.⁴ This leads to configuration management, training, and funding problems just to maintain the status quo. Third, both the early

airlift and IT fields lacked enough “pilots and maintainers.” To solve this, the services have hired outsourced expertise exactly the same way General Tunner outsourced maintainers in the Berlin Airlift.⁵

DEFINING THE CHALLENGES

Introduction

The U.S Air Force added cyberspace to its mission statement on December 7, 2005 and developed a cyber-based command, the 24th Numbered Air Force. By recognizing the need for this new command in modern warfare, Air Force leaders must also recognize how information technology and communications system management must evolve with the new organization as well. In addition, the DOD also formally recognized our nation’s technological evolution and established a new joint cyber command, USCYBERCOM, to combine service cyber missions into an integrated service for national policy. Therefore, effectively organizing, training, and equipping Air Force cyber forces, using a SPO construct for management constitutes a relatively more efficient and effective contribution to the nation’s global cyber effort.

Research Scope

The end-goal of this research paper is efficient management and dissemination of information to the strategic, operational, and tactical levels of the DOD. In researching this very ambitious and broad goal, three basic items kept appearing as the central pieces necessary to reach the end-goal. On the macro-level, system acquisition and architectures, on the intermediate level organizing structures for mining data and retrieval, and on the micro-level metadata tagging of individual information items.⁶

These three areas exist and are currently dealt with by a variety of existing Air Force divisions, directorates, agencies, and organizations to varying degrees. However, the essence of

this paper is to advocate integrating these areas into a single SPO organization to improve the overall effort. Within these three areas, it is necessary for this paper to focus on the macro piece first, because it establishes the basis for reaching the intermediate and micro-level goals. These areas have a long history, and should continue to develop in a parallel with one another; nevertheless, they need to come together under a united organization with a single vision to centrally control and achieve the end-goal of meeting DOD Standard 8320.02, which is making relevant data readily available to decision makers and war fighters.

Research Questions

This paper proposes a cyber SPO as an initial solution for the following questions:

- 1) Who says it is broken?
- 2) How does having a cyber SPO fix the Air Force's compliance with DOD Standard 8320.02?
- 3) What are some of the existing IT platform issues?
- 4) Why should the Air Force accomplish this bold effort?
- 5) When should the Air Force implement a cyber SPO?
- 6) What are the cyber SPO gains?

Defense Science Board Task Force Findings

The 2009 Defense Science Board Task Force (DSBTF) on DOD Policies and Procedures for the Acquisition of Information Technology examined the challenges facing the DOD and came to the following conclusions. Information technology systems are critical to national security, the DOD is unable to “effectively acquire IT systems,” because its acquisition process is not acceptable, thus affecting policies, processes, roles, and responsibilities.⁷ The task force

“believes there is a need for a unique acquisition system for information technology,” and the current process is “too cumbersome and long to fit the needs of many systems that require continuous changes and upgrades.”⁸

The DSBTF, identified nine IT environmental areas of concern technology change; disaggregated architectures; connectivity, size and complexity; vulnerability; cost; human resources; foreign supply and time. These IT issues transcend the DOD level through the services down to their operational and tactical levels. The proposed cyber SPO would address these issues from the Air Force level upward, and it serves as the downward focal point for operational and tactical issues discussed later in the paper.

Why is this IT acquisition process broken? According to the DSBTF report a primary barrier is “experience proven leadership and incentives (or lack thereof) to alter the behavior of individuals and organizations,” in which the participating entities “assumed they had responsibility to stop [or perhaps continue] programs that are unable to fully satisfy their concerns.”⁹ As a service level example, many commands developed administrative information workflow solutions to track performance reports, decorations, etc; yet service wide processes varied by command with each favoring a different process to accomplish the same administrative tasks. In recent years, multiple commands began implementing solutions such as Microsoft’s SharePoint and Community of Practice (COP) websites to great effect. A cyber SPO could serve to speed up implementation processes on similar, future developments. More importantly, it saves the redundant costs and man hours of multiple solution development.

Metadata Explained

In 2008, the Office of the Secretary of Defense formally structured its net-centric data sharing in DOD standard 8320.02. The essence of the standard establishes the need for a metadata hierarchy to manage lower level data within large volumes of existing data. For familiarization to the uninitiated, metadata is similar to an electronic tag on livestock, which has all of the information about the animal, herd, location, etc.

Metadata Example

Imagine billions of animals (products), in many countries (communities), on millions of farms and ranches (facilities) in millions of pens (locations). With these information tags, managers and customers (users of data) can search out the products they desire quickly and efficiently then transport the products from other facilities and locations to their locations to meet their needs (requirements). In order to operate the tagging system must be established, standardized, continually managed, and users must be organized, trained, and equipped to use the system. They must also agree on the system's rules of engagements or constructs between users, which requires governing bodies at global, national, state, etc...local levels.

Air Force Metadata Example

Once a SPO is organized and hardware and configuration management principles are stable the Air Force can build the file plans and information channels meeting the intent of DOD 8320.02. The Freedom of Information Act of 1974 (FOIA) is an excellent case for a benchmark in the DOD 8320.20 effort.

Currently, there is no robust capability for a linked, service-wide FOIA file search capability. The current method requires several manual levels of search, clearance, redaction,

and finally release. All of this must occur and redundantly cycle between different Air Force disciplines, public affairs, communications, security classification personnel, legal offices, and the information (content) owner until resolution and release via public affairs. Unfortunately, communications personnel, as an extra level of bureaucracy, manage the FOIA process, but need to focus on building systems and capabilities to meet DOD standard 8320.02. With SPO managed hardware, naming conventions, and structured file plans automated searches using metadata would speed searches and quickly identify eligible products related to the FOIA request. Additionally, the FOIA process would be shortened 20 percent by eliminating the need for communications office involvement.

Complex Metadata Example

A more complex example is the collecting, processing, analyzing, and dissemination of operational information for the intelligence community. This process is several magnitudes greater than the simple FOIA or any other administrative example.¹⁰ However, the processes and capabilities from a system and data management perspective are relatively the same albeit more complex.

Cyberspace Manning

As the Air Force reduces its communications workforce, Air Force Specialty Code 33S, to less than 2,000 Airmen in 2010, it is necessary to become more efficient in its force organization, training and equipping of cyber capabilities. A communications SPO could consolidate cyber force training and asset management to counter increasing foreign capabilities from countries expanding their IT systems, information warfare doctrine, and capabilities. For

example, in 1999 the Chinese military already had two brigades (about 5,000 people) dedicated solely to computer attack and defense forces.¹¹

SOLVING CHALLENGES

Cyber SPO Creation

Why manage IT like a weapons system? For approximately the past 20 years, the growing internet years, acquiring communications in the Air Force and specifically information technology hardware has consisted of many ad-hoc, disparate programs, which rely on discretionary funding on many levels to keep missions effectively connected. Perhaps discretionary funding was a good fit for lower level, end-user support items (personal computers, printers, etc), and administrative functions in the past. Furthermore, each command's individual programs and discreet acquisition efforts kept long haul communications, airborne, space-related, and other big system architectures sustained.

These systems are now increasingly interdependent on one another and growing in magnitude of complexity, thus the need for centralized governance. Furthermore, administrative system capabilities now integrate directly into operational mission sets causing overlapping dependencies. For example, flight mission planning accomplished with the Federal Aviation Administration via Falcon View software over unclassified networks. Another example is logistical support around the globe accomplished by database systems connecting via standard internet, and web page interfaces sharing data with commercial vendors, contractors, and other government organizations.

Therefore, the unit issued laptop has become more than an administrative tool for performance reports and decorations. It is a mission enabler, which develops mission route

plans, links Air Force flight information to the Federal Aviation Administration, and creates and approves travel orders, costs, and travel reservations on civilian airlines.

SPO Justification and Roles

Even before the proposed creation of the AFCYBER and USCYBERCOM, IT systems and professionals needed consolidated and standardized methods for procuring IT systems while managing quick growth. Now the DOD services need efficient IT management even more for two reasons. First, economic downturn typically results in reduced DOD budgets. Therefore, the DOD services need to posture all systems resources for trade-offs between capabilities, reduced funding, and mission requirements. IT systems are arguably one of the largest disbursed costs across all cross-functional communities within the Air Force; therefore, a single point of organization could reduce the impact of these budget reductions. Second, data sharing between services, governmental departments, and non-governmental organizations requires systems to have configuration management and standardization. Managing both of these, architecturally, requires the total effort to reside under a single umbrella of control similar to any weapon platform. These build the macro and intermediate pieces, and then we can address formal data sharing standard set by the DOD on the micro level.

SPO Benefits

This SPO and product structure effort limits unnecessary exposure of classified information to those who have the need-to-know by reducing a layer of bureaucracy. The new structure enables timely destruction of superseded information, and it provides faster solutions with reduced manpower. Furthermore, the DOD 8320.02 and SPO effort addresses future FOIA needs due to the Air Force eliminating approximately 50 percent manning reduction in the

communications career field between Presidential Budget Decision (PBD) 720 in 2007 and the upcoming Personnel Services Deliver Memorandum (PSDM) 09-65. This is only one simple example, in one service illustrating the need for the DOD standard and the SPO to refine and leverage current IT capabilities.

Current Challenges

As of the publishing of this document, the Air Force is reviewing its new numbered air force (NAF) and its joint role with Cyber Command. The primary issue, currently under review, is upgrade the USCYBER commander rank from Lieutenant General to General so cyber forces have top representation for cyber resources equal to other platforms. Secondly, there can be a real dilemma in applying aircraft and maintenance operation jargon and methods to cyber issues for the mere purpose of making them “fit” in operations. You can train, equip, and manage IT *like* a weapons platform; however, the medium is different for operations with complex challenges (legal, policy, treaty, environmental, etc...) not faced by physical assets.

Cyber Operation Comparison

One example where cyber operation characteristics do and do not translate well into current Air Force operational language is as follows: A “time to acquire target” can be measured as 300 milliseconds; however, that is where the physical asset and cyber asset depart similarity. Acquiring a target is measurable, but the target might not be able to be “eliminated” or “precisely engaged,” or persistently attacked due to cyber boundaries such as political issues, international policy, treaties, standards, and existing laws.¹² Speed of commanding a network is simply too fast for immediate human reaction, whereas a physical attack has clear-cut consequences,

borders, and responses.¹³ Second example, how do you accomplish battle damage assessment or isolate a single combatant in a virtual environment.^{14,15}

A third consideration is the possibility for cyber operators to fly a “block 30” network, similar to the physical flying of a “block 30” spiral modified aircraft. The initial contention would be a “no” from the offensive point-of-view, simply because different organizations, both friendly and hostile, use a widely varied mix of resources, talents, hardware, and software to accomplish their tasks.¹⁶ The evolving nature of virtual targets precludes a “strict flying of a cyber asset” with a payload of established and tested capabilities to launch. This changes the nature of find, fix, finish, engage and assess (F3EA).

On the opposite side of the same spiral modification, the network defense side of the network mission could benefit from mass standardization; this theoretically limits a network to known vulnerabilities, allowing known weak points to defend versus networks comprised of myriad systems with layers of exploitation vulnerabilities. Again, this illustrates the differences between virtual assets compared to physical assets. The policy makers and international bodies have yet to constitute what an “attack” is in cyberspace, yet flying and space assets have a host of governances. This type of activity will require politicians, international communities, and nations to define what sovereignty is in the cyber realm, before military operators can create and train on their rules of engagement, offensive or defensive, in cyberspace.

IMPLEMENTATION

Introduction

Operational issues, between aircraft and cyber may differ, their physical management, system development, and procurement processes can be very similar. Implementing a cyber SPO would be the first step in managing cyber assets like a weapons platform. The initial functions of a new cyber SPO would begin to fix the macro area items first then incorporate the parallel efforts of intermediate and micro items. The phases and timing of these elements require further study to build an implementation schedule for the SPO to begin its efforts. The macro-phase would truly be the most ambitious. It requires the DOD to establish several key technical capabilities for the Air Force and its fellow services to use for creating a complete joint system view of the existing technical architectures. First, by having a single enterprise level, web-based tool each DOD component can build a common sharable view of their assets from the smallest elements to the largest agency. Secondly, on the intermediate level file structures and databases can be standardized and integrated to enable better searches of existing information. Lastly, metadata tagging vast volumes of information, particularly older non-digital information, will take time. Accomplishing this can occur through attrition of newest to oldest information and as pervious information is requested. Moreover, metadata tagging has the potential to strengthen classification adherence, auditing, and timely information destruction in addition to its established search capabilities.

Initial Macro Level Issues

The first macro level issue a cyber SPO would address is documentation of current cyber assets. In researching this topic, it appears the DOD components, their subordinate commands, support agencies, and lower level organizations all use different tools to document their architectures. Some of the tools are compatible and some are completely proprietary. The point

is updating system architecture documents, in a common, standardized tool, must occur for proper configuration management, with the same rigor as aircraft modernization. Without this discipline coalescing into a single effort, cyber forces cannot efficiently limit vulnerabilities, modernize deficient systems nor can a service track the true cost of its inventory and present and future requirements.

The second macro-area is related to the first, it is the acquisition and communications requirement development. The DOD's cyber resources need to have a single web-based project management capability for managing systems workflow requirement resource. Many of the aircraft SPO use Microsoft's Project on an enterprise level and Air Combat Command uses Project Workflow Requirement Resource (PWRR) to manage technical requirements. Once set up across the DOD enterprise, the lowest level units could build requirements and forward them through their approval processes to satisfy operational and administrative needs. The cyber requirement checklist in Appendix A serves as a rough guide for what a basic requirement template might contain. Once developed Air Force, major commands, agencies, wings, groups, etc... could formally review the requirement then measure the submission's "strength" for the corporate funding process and determine its overall prioritization. The requirement strength indicator (RSI) template in Appendix B could be an on-line metric and method for distinguishing many requirements and ensuring operational need truly come to the top leaders for review. It allows, commanders and resource advisors to prioritize and sort complex technical issues while keeping units informed of where their requirements are in the process. The first two macro areas architecture and requirements should dynamically link to provide a before-and-after or "as-is" and "to-be" view into a system; thereby displaying what capabilities exist and what is needed for the investment made. Additionally, with these macro-items linked large phased project across

multiple funding years have continual status and visibility in corporate, planning, and mission processes.

The third macro-related area concerns funding and it ties into the first two areas. Currently, broad categories of program element codes (PEC) allow for purchasing ambiguity under some generic codes. To correct that area, specific PEC and program element management (PEM) codes could be designated for the different Global Information Grid (GIG) segments and perhaps even sub sections (discussed in SPO Structure section below). With well-defined codes, services can improve and solidify budget and equipment replacement schedules for aging equipment while discovering the real costs of systems. Sorting through the codes, in a web-based requirement system will establish trends to help manage information technology and system costs at all levels. This leaves a commander's discretionary funds for unscheduled mission related needs and it allows cyber resource managers a method to consolidate known requirement costs into annual initiatives helping wing-level and major commands better manage system costs. This also saves man-hours at the lower unit levels, because equipment replacement is a known factor and the unit will not need to develop or defend a requirement and it will not need to fund the requirement from its funds.

The last macro-item concerns the use of smart client server based computing. If the services re-investigate this technology they can cost-effectively eliminate many maintenance issues, hardware tracking responsibilities, individual user software licenses, and security vulnerabilities at the unit level. Smart clients help the squadron level and below greatly because the Air Force no longer has communications professionals to accomplish these duties in the units. As manning decreases and operational tempo increases smart-clients could reduce these demands, which are now placed upon the remaining core squadron members as additional duties. These members

must divert time from their operational duties to deal with unexpected system challenges. Smart clients, enable the Air Force to manage their administrative IT network like an aircraft system by controlling costs, configurations and improve the mission readiness rates. Initial costs to change the system from current “fat” client to smart-client could be mitigated by using a phased approach and once fully in place the Air Force could divert unused administrative system funds to higher priority communications requirements. According to an Advanced Technology Labs presentation at the University of California-Berkley, smart clients offer the potential, comparative annual savings as follows: An 80 percent reduction in maintenance costs, a 25 percent capital cost savings, 23 percent reduction in operational cost; combined studies show these enterprises save around \$50k a year for every 1,000 thin clients in operation.¹⁷ If accurate, this represents a monetary saving of 16.8 million-dollars per year, based on a 335,000 Air Force population, on non-secure networks and potentially another \$5M on secure networks (assuming secure networks cover 30 percent of the Air Force population). Moreover, it assists the Air Force’s communications career field, which is approximately 45 percent smaller after Presidential Budget Decision PBD-720 in 2007 with further pending cuts scheduled in 2010; plus, it keeps operators focused on mission issues not on additional duties. Across the DOD’s total population of 3 million personnel, the same effort could save additional man hours and 129 million dollars (approximate) in network costs.

Initial Intermediate Level Issues

The Air Force uses the Air Force Records Information Management System (AFRIMS) to organize its file structure and determine generically what is in the file and manually indicate when file destruction is needed. This is a great program for local file structures but was built for traditional file cabinet management of records. Placed on-line “CYBERRIMS” could take its

services to a much higher level of effectiveness by integrating the digital file structures it creates into a dynamic environment such as the DOD Metadata Registry (DDMR). With a dynamic, web-based file system and using metadata in the contents, users could use search engine technology to locate unit and unit-related information faster and even have automated prompts for timely classification and information review and destruction of specific items and folders. The web-based system could also assist in traditional physical file management, by having searchable indexes that point to a physical file's location and contents. Current file record managers could create DDMR standardized file structures and have commands, wings, and agencies populate them across a given time frame. Once the structure is in place file backup plans could be automated to reduce the risk of lost information, similar to the commercial file backup technology used by the Carbonite © or Mozy © companies.

Initial Micro Level Issues

Both Defense Knowledge Online and the DOD Metadata Registry are great initiatives for the micro-level, where data tagging specialist can imbed and search data using the development and retrieval tools at their disposal. The key for both of these web-based services is to get everyday users to know these services exist for their community of interest and organizations, and then get them involved in tagging information, and having the benefits advertised to encourage greater use. Increasing visibility is a key element for these portals making them integrated into everyday usage.

With smart-clients, and searchable web-based file systems the Air Force can save funds on systems, more importantly it can keep its operators on mission with better administrative support. As mentioned before, this effort alleviates the transitional and shrinking communications career field by pulling communicators away from lower level administrative

duties and asset tracking systems and moving them to higher priority mission related systems and efforts.

SPO Structure Recommendation

So how does a SPO meet DOD Standard 8320.02? The opportunity for the Air Force exists, in these early phases of establishing AFCYBER and USCYBERCOM, to organize itself in a manner benefitting the ultimate goal of transparently sharing data. The SPO construction should organize into the functional areas or segments of the Global Information Grid (GIG). This structure is an easy model for visually conceptualizing a complex system of systems and it focuses resources and leaders on exactly where a requirement is in the GIG or system. By establishing GIG segment framework in the cyber SPO, leaders can forecast costs with mission impacts, organize equipment, train skill sets, and apportion Airmen to meet Air Force and DOD mission needs. Below is a hypothetical framework for a cyber SPO to meet Air Force, joint cyber forces, and Office of the Assistant of Defense for Networks and Information Integration, DOD Chief Information Officer, or OASD (NII)/DOD CIO needs for communications resource management:

1. GIG Segment 1 - Enterprise Level

- a. Air Force Cyber Liaison Office –guides Air Force efforts to meet DOD policy, continues to link Air Force communications community to DISA, NSA, DIA, and other national offices.
- b. Air Force Cyber Metric Office – establishes web-based metrics concerning all cyber resources, status, costs, mission efforts, etc. This office builds an annual cyber accountability report as a single point of information for senior

leaders on Air Force cyber forces and their contributions to the DOD, joint community, and national defense.

- c. Space-based communications networks – links space resources to customers
 - d. Airborne communications systems-serves Airborne resources to communities
 - e. Theater Operational/Tactical communications networks – serves the operations community and special operations
 - f. Circuit management and cryptologic services – consolidates circuit management into one office, spectrum management, and leads Air Force cryptology issues and resources.
 - g. Architecture and Configuration Management – manages all communications architecture resources, metrics and related issues
 - h. Communications Requirements Office – oversees communications acquisition, project management capabilities, reviews, and prioritizes funding for large requirements, allots communications budget resources at all levels
2. GIG Segment 2 - Installation (Campus) level liaison and management of wing and agency level issues and requirements
 3. GIG Segment 3 - Facility (Local) level – Serves the focal point for group and squadron levels communications issues; builds and enters requirements, updates architectural documents.
 4. GIG Segment 4 – Traditional Services – Serves as wing level and below liaison and planning and implementation element for airfield systems and communications resources, local radio, telephone, local support contract efforts, and requirements.

5. GIG Segment 5 – Classified customer level – serves at the facility level for classified networks
 - a. Unique networks (other agency, intelligence, medical, and legal)
6. GIG Segment 6 – Information Management Office (office automation, file management) – manages and leads intermediate level issues concerning workflow management initiatives; file management, migration of information onto web-based sources, metadata tagging efforts, and provides metrics on relevant issues. This office exists at the enterprise, installation, and facility levels.
7. GIG Segment 7 – Cyber Standards, Evaluations, and Training – standardizes, coordinates, tests, and measures all communications and information training resources and activities. Provides metrics on workforce, (civilian, military and contracted) effectiveness

In this SPO construct, each of these GIG segments has its own unique set of PEC and program element codes to clarify budget costs and projections.

Cyber SPO Feasibility and Alternatives

As mentioned before many of these organizational elements already exist they only require a unifying effort to pull them into a formal cyber SPO. Where would the cyber SPO physically reside? Ultimately, that decision would have many political and technical decisions, and would need a formal study to allocate resources for such a large endeavor. Several facilities already have large communications and information presence now and may be the best places to place a representative SPO. As an alternative, in the near future with far less cost, it is feasible to build a virtual SPO in the communications and information community of practice. Air Force leaders could begin aligning policies and support documents to reflect the new cyber SPO

construct. This is excellent timing because cyber SPO creation now fits in well with the Air Force's current effort of migrating the Communications and Information, 33S Air Force Specialty Code (AFSC) to the new cyber force –related 17D AFSC. By planning and accomplish this effort as a virtual structure the Air Force will save funding, yet have the requirements and organizational elements finalized before establishing a physical structure.

Continuing Research Areas

This research paper merely touches on the basic, initial items a cyber SPO should address within the context of America's newest, cyber forces AFCYBER and USCYBERCOM. The items in this paper are based on both intellectual investigation and the author's experience with communications system procurement; however, this paper cannot not answer all of the fundamental challenges faced by the cyber community, the topics are very broad and across a wide spectrum of expertise. The Air Force needs a series of formal studies to begin formulating an actual cyber SPO.

As a recommendation, each part of the macro, intermediate, and micro levels, the GIG segments, and its sub components, requires formalized study conduct with the related subject matter experts to determine how a real cyber SPO is structured and how the functions would integrate together. These studies could discover true costs, returns on investment, define who would perform the functions, and establish the policies and authority to make the cyber SPO useful. Some other areas for potential study and research:

- Use of contracted commercial email services for non-secure email support
- Migration of file plans into a Web 2.0 environment, DDMR, etc...
- A DOD sponsored, web-based cyber requirements system

Air Force Example Revisited

Lastly, a study for revamping the Freedom of Information Act (FOIA) process is needed to speed the process and migrate it away from the disappearing 33S career field. Currently, as shown in figure one, the process involves communications and information (33S) organizations receiving direct, outside requests from the public for information, then through a series of public affairs reviews, legal reviews, subject matter expert (SME) reviews, and redacting (done by 33S with SMEs) iterations occur followed by information approval or disapproval processes for release. Finally, a customer notified by the 33S community receives the resulting outcome of the request. With the 33S career field migrating to the operational 17D, cyber force there is an opportunity to shorten the FOIA response cycle and increase its efficiency by removing the former 33S elements. In the new construct, public affairs would lead the new FOIA process by accepting incoming requests from public sources, along with releasing results to the public. In the process, SMEs are responsible to redact their related information, then legal services reviews the final information package for commanders and returns it to public affairs for release or notification of information denial to the requester

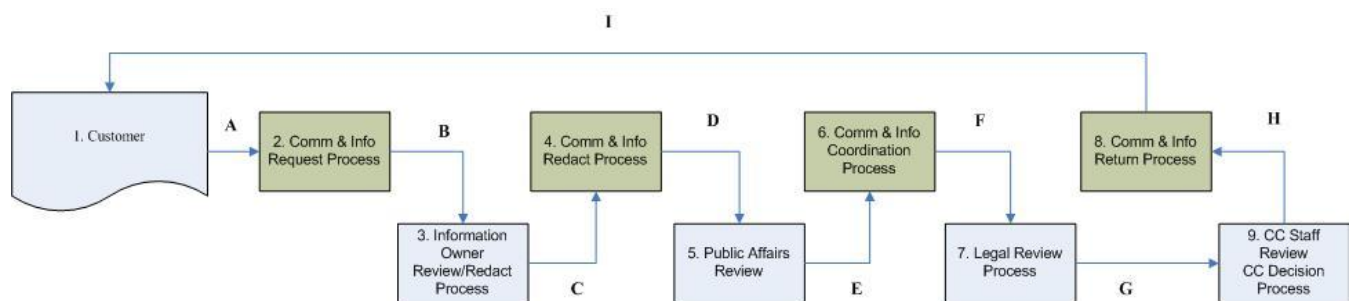


Figure 1- FOIA Current Process

Figure two represents a streamlined process utilizing metadata tagged information and a reduced organizational structure. This structure holds the potential for, a 20 percent, a five to four organizational reduction in career field usage and a 50 percent, 8 to 4 step reduction in

process time. A formal study could determine the thousands of man-hours and costs saved in reducing this complex processes to its most efficient form. Obviously, once a defined and mapped system, file plan, and properly metadata tagged information exists FOIA request searches could be greatly sped up probably from months to days.

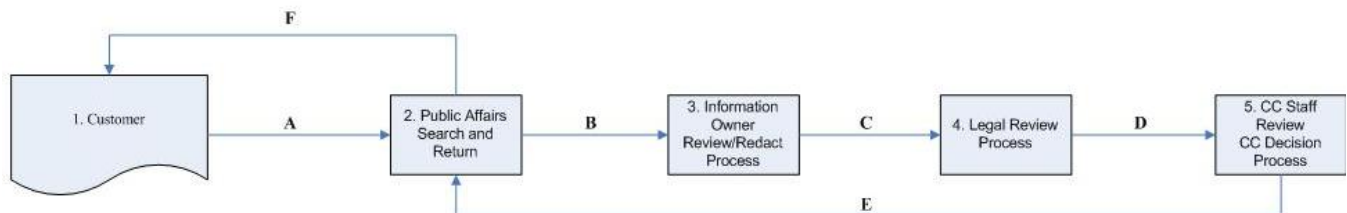


Figure 2 – FOIA Streamlined Process

This FOIA improvement is only one example of how a cyber SPO provides a structure and process improvement capability to meet DOD Standard 8320.02, then provide man-hour and cost savings for a real-world example.

CYBER SPO IMPACT ON DOD 8320.02

Future Air Force ability to meet cyberspace missions and satisfying DOD standard 8320.02, depends on the service organizing training and equipping via a communications special program office. Without a cyber SPO, the expectation is the Air Force will have an arduous time meeting its informational, cyber system needs, and its obligation to the Department of Defense's need for data sharing in the information age. Creating this single, cyber SPO the Air Force can concisely manage over two billion dollars worth of existing communications systems and IT related requirements including DOD 8320.02 efforts.¹⁸ Beyond the annual funding allocation of \$2B, is the need to manage these assets because they connect over 335 thousand Air Force employees with approximately three million DOD members and beyond. A SPO also aligns the

Air Force's cyber force with the new "Department of Defense Strategic Acquisition Platform" for Information Technology initiative.¹⁹

CONCLUSION

Without the foundation this cyber SPO provides, the finite, tactical level effort of metadata tagging all relevant and available information cannot occur on a large scale nor is the metadata tagged information accessible without a well-defined system and a standardized file structure. Once the Air Force, establishes the cyber SPO, brings procurement and governance of communications systems in diverse communities, in varied facilities under a single governing body, we can manage our electronic products at lower levels, the locations and facilities, where they reside. Furthermore, by formalizing the acquisition and purchasing of all communications systems, including information technology (IT) systems, under the SPO construct the Air Force can meet the intent of DOD guidance on Standard 8320.02 and on acquisition of federal IT systems.

The end-result is a special program office managing and funding the cyber enterprise the same as any other platform and in the same manner aircraft and space systems have done for decades and it allows the Air Force to share critical, timely information with the DOD and its global partners.

ENDNOTES

- ¹ Rattray, *Strategic Warfare in Cyberspace*, 293.
- ² Hughes, *Rescuing Prometheus*, 75-79.
- ³ Tunner, *Over the Hum*, iii
- ⁴ Ibid, 26.
- ⁵ Ibid, 169.
- ⁶ Thuraisingham, 1-65.
- ⁷ Defense Science Board, *Acquisition of Information Technology*, i-xix.
- ⁸ Ibid, 4.
- ⁹ Ibid, 37.
- ¹⁰ Lowenthal, 65.
- ¹¹ Thomas, *Dragon Bytes*, 57.
- ¹² JFQ issue 46, General Cartwright Interview, 48.
- ¹³ Alberts, *Network Centric Warfare*, 163.
- ¹⁴ Ibid, 216.
- ¹⁵ Lowenthal, *Intelligence: Secrets to Policy*, 249-250.
- ¹⁶ Alberts, 219-220.
- ¹⁷ Advanced Technology Labs, 22
- ¹⁸ DAF Procurement, F-22A.
- ¹⁹ Boland, *Military Receives Outline to Revamp Acquisition*, 44.



BIBLIOGRAPHY

- Advanced Technology Labs, Thin Client Computing Solutions Briefing, Developed for the University of California Berkley, <http://www.ocf.berkeley.edu/.../ATLabs-ThinClient-Etisalat-finalv3.ppt>, (accessed 3 April 2010).
- Boland, Rita, "Military Receives Outline to Revamp Acquisition," AFCEA Signal Magazine, November 2009, http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2106&zoneid=278, (accessed 3 April 2010).
- David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, Sun Microsystems Federal, February 2000.
- Defense Science Board Task Force, *Department of Defense Policies and Procedures for the Acquisition of Information Technology*, Washington DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, March 2009.
- Department of the Air Force Procurement, Air Force Other Procurement FY11, page F-22A. <http://www.saffm.hq.af.mil/shared/media/document/AFD-100128-066.pdf> (accessed 3 April 2010).
- Hughes, Thomas P. *Rescuing Prometheus: Four Monumental Projects That Changed the Modern World*. New York, NY: Vintage Books, 2000.
- Lowenthal, Mark M. *Intelligence From Secrets to Policy*. Washington, DC: CQ Press, 2006.
- Rattray, Gregory J. *Strategic Warfare in Cyberspace*, Cambridge, MA [or London, U.K]: MIT Press, 2001.
- Thomas, Timothy L. *Dragon Bytes, Chinese Information War Theory, and Practice*. Fort Leavenworth, KS: Foreign Military Studies Office, 2004.
- Thuraisingham, Bhavani. *Web Data Mining and Applications in Business Intelligence and Counter-Terrorism*, Boca Raton, FL: CRC Press, 2003.
- Tunner, William H. *Over the Hump*. Washington, D.C.: Air Force History and Museum Programs, 1998.
- Smotherman, Jeffrey D. Interview with General James Cartwright, NDU Press, Joint Forces Quarterly, issue 46, 3rd Quarter 2007.

APPENDIX A - CYBER REQUIREMENT CHECK LIST TEMPLATE

This cyber program is a requirement-driven funding source for improving communication infrastructures. However, the program itself does not do the prioritization and justification of these requirements. The related program manager must review these requirements first, then release them via web-based methods to the local A2, A3, A6 directors, then to the A5, and financial communities for entry into the Cyber Corporate Process. The program manager, to ensure the requirement documents are complete for entry into the Corporate Process, uses the following checklist:

Part 1-General Items

Unit: Unit/ office symbol (from the drop down menu, based on roles and permissions)

Priority: *leave blank*

Title: Descriptive title of requirement (example Network Cable Replacement Initiative)

Unfunded Amount: Type/Amount in \$K (Example BA-04 \$300K), if over \$1M finance will require an economic analysis

Baseline Amount: The amount in \$K of requirements submitted in the current FY FINPLAN (example BA-04 \$0)

Panel: *leave blank*

PE –Get from your Resource Advisor (Example 310XXF)

AFEE (EEIC) – Element of expenditure indicator code, get from your Resource Advisor (Example 592, make sure it is related to the proper GIG segment)

Part 2-Initial Description Items

The initial description items, ‘Narrative Justification’ and ‘Impact if Not Funded’ should both fit easily on one page and be no more than ten sentences each. These two introductory items for your requirements are typically placed in presentations and databases and must be concise. Details are spelled out in the supplemental section.

Narrative Justification:

1. Ten sentences or less (details are spelled out in the supplemental area)
 - a. Know your audience—don’t write using jargon and spell out acronyms
 1. The FM and A5 communities require clarity and usually don’t know your career area thoroughly
 - b. Needs to be concise for presentations and database use
 - c. Is this a stand-alone requirement or part of a bigger project
 1. If part of a bigger project see 4.c below

2. Describe who the requirement serves (at least one of the following as a minimum)
 - a. Customers or community of customers (quantify)
 - b. End users (analysts, pilots, maintenance, personnel, etc)
 - c. Individual recipient (state how the requirement satisfies tasks, etc for this persons job)
3. Tell what mission and possibly related operations are tied to the requirement
 - a. Example ...our PIE –IN-THE-SKY mission along with Operation BIG SLICE
4. Short description of the capability needed by the unit
 - a. Service
 - b. Process
 - c. Product
 - d. Resource
5. Describes the condition which created the need
 - a. Mission increase
 - b. Technological change
 - c. Funding fell short on another program
 - d. Deficiency of current service, process, or product
6. Quantify what the establishment, improvement or enhancement will provide
 - a. What is the end-state of satisfying this requirement
 1. Tell the FM and XP communities what will fixed
 - b. Percentage of improvement
 - c. Number of... will provide extended service
 - d. Establish this service fixes_____ deficiencies

Impact if Not Funded:

1. Concise (10 sentences or less) for presentations and database use
 - a. “Mission will fail” and “mission stoppage” are bad comments to use in requirements and rarely true.
 - b. Coherent statements written for A5 and FM community
 - c. General terms like GWOT (Global War on Terrorism) must show a direct link to your mission
2. Quantify what happens to the mission if this capability is not funded
 - a. Describe which part of the mission/operation suffers
 - b. How much will it suffer?
 - c. Detail the degree of suffering
 - d. Reference violations incurred if not funded
 - i. Inspector General report number
 - e. Support items:
 - i. Laws, Presidential Orders, governing body direction
 - ii. Instructions (DoD, Joint, AFI, etc)
 - iii. Downward directed

P.O.C: Name, rank, unit/office symbol

Part 3 Supplemental Information

The Supplemental Section is where you spell out the details of everything you mentioned in the above sections. Additionally, this section has the extended write all of the attachments and source documents, which bolster your requirement's chances for funding. Keep in mind the level of detail in this section typically determines your prioritization and ultimately your funding, particularly, if the requirement is high profile or a large funding amount.

(1) Sponsor/Submitter: Name, Grade, or Rank, position or parent organization

(2) New Initiative (Yes/No): Self-explanatory

(3) Submitted by: fill in and answer the following questions

1. (Wing/center)_____to HQ AIA as an FY (applicable years)____ AF POM, CCP or GDIP initiative? (Yes/no)____
2. Approved by HQ AIA for FY (applicable years)____ AF POM, CCP or GDIP submission to SAF or AF/XOI? (Yes/no)____

(4) Links to Validated Planning Documents: Show any documents supporting the need for the requirement. This section should be supported by item (7) the expanded justification.

1. C4ISR documents
2. 3215 or Contracting Documents
3. Architectural Products
 - a. Diagrams and Drawings
 - i. Baseline "as-is" drawing
 - ii. Planned "to-be" drawing
4. Laws, Mandates, Executive Orders, etc (highlight applicable sections)
5. Professional Products
 - a. Engineered solution reports
 - b. Cost analysis and breakdown reports

Example:

AFMAN 37-139, Records Disposition Schedule; AFI 33-322, Records Management; AFM 37-123, Management of Records; AFI 37-138, Records Disposition—Procedures and Responsibilities; DOD Directive 5015 STD, DOD 5400.7/AF Sup, Freedom of Information Act; AFI 33-332, Privacy Act; Executive Order 12958, Section 3.4

(5) Last Date Funds Can Be Received and Executed: The latest date the unit can act on the requirement if funded (example 10 Sep XX)

(6) Requirement is: ____Mission Critical ____ Mission Impact **X** Mission Enhancement

Mission Critical: total mission collapse if not funded

Mission Impact: severe, moderate, or light mission degradation

Mission Enhancement: partial or total mission improvement

(7) Expanded Justification:

This section is where the hard-hitting detailed items of the requirement are spelled out. This section expands on the narrative justification and carries the most weight in justifying the funding of your requirement and the requirements final prioritization. The Expanded Justification narrative should address the following topics, as a minimum, for a complete requirement picture:

1. Restate mission supported by the requirement
 - a. (i.e. supports Operation BIG SLICE, etc)
2. Restate if requirement was identified as part of an official report
 - a. Inspector General (IG) report,
 - b. Infrastructure Assessment Team (IFAT) report
 - c. Downward directed program.
3. Restate policy documents supporting the requirement.
 - a. Federal (i.e. required due to Clinger –Cohen Act and AF CIO)
 - b. Department of Defense,
 - c. NSA, DIA Business Plans, etc..
 - d. Air Force (i.e. required due to AFI XX-XXX)
4. Explain any other the issues/items the requirement might provide
 - a. Mission enhancements
 - b. Alternate uses
 - c. Metrics and figures

5. Include any additional costs
 - a. Setup
 - b. Shipping costs
 - c. Removal of old equipment
 - d. Other relevant funds needed to install the requirement.
6. Restate any important factors
 - a. Legal ramifications,
 - b. Potential loss of life, injury to personnel,
 - c. Damage to existing equipment, etc...
7. Include detailed architecture products System View (SV-1, SV-2), Operational Views (OV-1, OV-2) and other appropriate architectural products; plus, any applicable documents such as an AF Form 3215, PWRR document.

(8) Provide a cost breakout of project funding segments:

1. Submit a detailed spreadsheet of items to be purchased for the requirement. It must add up to your requirement total
 - a. Products
 - i. Hardware
 - ii. Software
 - b. Services
 - c. Resource

If phased, explain the order your unit can satisfy the requirement as funding becomes available. If the project can be accomplished in phases, break out the order and minimal cost of each phase. In addition, if phases need to be completed in order state the order for example, a system planning or design phase occurring before an equipment-purchasing phase. ***Do not assume phases will be accomplished in order; funding requirements are sometimes accomplished out of order.*** You must tell the finance and contracting requirement reviewers if the order can be single source or not.

If execution order is not important, meaning Section 13 will be answered no, then a general narrative such as the example below could be used.

(9) Related Projects or Systems: Show conjoined systems or related initiatives

1. Laundry list items

(10) Facilities, Mechanical, and Electrical Requirements:

This section identifies physical items (such as power, construction, etc...) needed to complete your unit's requirement and ultimately satisfy your mission. This section is a flag for Civil Engineering requirements. If a work order has been put in for the requirement place the relevant order number and information in this block to show linkage between your requirements process and the CE initiative.

(11) Mission Supported: Specify which mission the requirement meets.

(12) Resource Requirements:

Place the amount needed for this requirement in the first FY UNFUNDED (column). Align the value next to the appropriate type (row) leaving the other cells at default values (\$0).

	FYXX FUNDED	FYXX UNFUNDED	FYXX FUNDED	FYXX FUNDED	FYXX FUNDED	FYXX FUNDED	FYXX FUNDED
3400	\$0	<i>\$300K</i>	\$0	\$0	\$0	\$0	\$0
3080	\$0	\$0	\$0	\$0	\$0	\$0	\$0
3600	\$0	\$0	\$0	\$0	\$0	\$0	\$0

(13) Can This Project Be Done in Phases (Yes/No): Yes.

This section relates to Section 8

(14) If Yes, Show Phases or Provide Minimum Funding Needed:

This section also relates to Section 8.

(15) Manpower Requirements:

	FYXX
Officers:	0
Enlisted:	0

Civilian: 0

(16) Approving Official: _____

Name, Rank, USAF, Director of Operations



APPENDIX B - REQUIREMENTS STRENGTH INDICATOR PROCESS

General

Why the Requirement Strength Indicator (RSI)?

- Approximately 80 percent of all requirements must be sent back for further correction, elaboration, coordination and resubmission.
- Interviewed several hundred years of experienced people and by asking new requirement writers what their frustrations were.
 - All at different organizational levels and stages of development

Current Status of the RSI Process

- Baseline standard established—improvements measured
- The parent organization Requirement Review Report sent out
 - Individual requirement score sheets
 - Explanation message & this slide show included
- Units see overall scores, but not each other's requirement info
- The RSI process/EOY accounting call bookend SB
- Supplemental data call (Suspense: Date) before final prioritization

Role Players in RSI Development

The following communities discussed this issue and played a role in the development of the RSI

- Plans and Programs (XP aka A-5, J-5)
- Director of Operations Staff (DO aka A-3, J-3)
- Financial Management (FM)
- AF Cryptologic Office (NSA)
- IT IS (AB23) at NSA
- Comm & Info (SC aka A-6, J-6)
- Civil Engineering (CE)
- Wings, Centers, Units
- A variety of others

Customer Response

Upon interview, SB Program Manager found that the customer overwhelmingly wanted:

- A single entry point for requirements
- Web-bases visibility
- Feedback in a timely manner
- Single requirement format
- Subjectivity mitigated
- A standardized way to gauge success/failure of a requirement
- Reduce time spent on writing/review
- Structured maturity in the process

Purpose of RSI

The RSI is a checklist method used to...

- Objectively review SENSOR BUS submissions
 - Check requirements for completeness
 - Establish a minimum threshold of information
 - Inform the customer – quantifies “strength” of the written requirement – provides a feedback mechanism
 - Answer critical questions for the DO and others...to establish a “true” priority
- Briefed last C&I Conference and in Aug 03 guide

How Does the RSI Work

- The RSI is a weighted check list
- 193 Items are looked at in three sections
 - General Items 12% of score
 - Initial Description Items 34% of score
 - Supplemental Information 54% of score
- Point system scaled to requirement size
 - Information needed is proportional to cost of submission
 - Not all checklist items apply -- N/A column nulls items
 - Raw score turned into % (actual pts / possible pts)
 - Allows comparisons of all submissions

What The RSI Metric Is NOT...

- The RSI is NOT...
 - Intended to question the validity of a requirement
 - A pass/fail grade for requirements
 - Simply measures completeness of submission
 - A scoring tool used for prioritization
- Operational prioritization is determined by the DO based on the written details
- A “complete” submission can better communicate importance– sets the stage for your operational need

RSI Benefits to the Customer

- Rules-of-engagement are established in a coordinated manner
- Clearly defines items, format and supporting documents required by requirement reviewers
- Collects all the relevant information in a forthright manner – reduces supplemental data calls
- Forces the question “Why is this important to the Director of Operations and what does it do for the mission?” and reduces the emphasis on “What I want from the HQ?”
- Matures requirement writers
- Helps build baseline documents for as-is and to-be planning, strategy and goals
- Quantifies probability of success of a requirement based on the amount of information provided
- Quantifies the ability/level of the Program to advocate for a requirement in an open forum and answer typical “critical” questions

RSI Benefits to Program

- Displays for all communities and customers, the “strength” of requirement documents
- First step to eliminate any perception of organizational bias—mission is the focus of SB

- Allows the SB to push requirements to other programs if applicable—w/o pushing workload
 - Stand-alone initiatives/roll-ups can be built/defended
- FY05 Baseline year for the metric—briefed at C&I Conference and in Aug 03 Guide

RSI Benefits to A-6

- Displays C&I relationship to Information Operations
- Matures funding process for nebulous “IT” items and networks
- Solidifies and links mission systems and information operations results
- Increases depth of knowledge of intelligence community requirements
- Baselines for as-is and to-be planning

RSI Benefits to FM

- Accounts for funding spent
- Breaks down cost by commodity
- Shows what funding fixed
- Shows direct correlation to mission and operations
- Provides traceability
- Baselines for budget planning

RSI Benefits to A-5

- Standardizes programs
- Shows what planning fixed
- Links mission and operations requirements and funding
- Provides traceability
- Standardizes historical information
- Strengthens baselines for existing planning (as-is)
- Strengthens requirements for future planning (to-be)

RSI Benefits to A-3

- Precious funding on-target with operational needs
- Matures planning & funding process IO systems and networks
- Accurately highlights the disjoint of operations if funding remains unsatisfied
- Helps intelligence community develop robust requirements sight picture
- Builds a requirement pyramid for congressional plus ups

Supporting Issues

RSI allows requirement reviewer to:

- Clarify what document items must be included in a “complete” requirement
- Clarify depth of explanation on items
- Convey Format compliance
 - Community specific (Finance, Plans, etc...)

RSI is a tool for requirement writers of varying experience

- Provides guidance for the beginning requirement writer
- Allows writer to know all the audiences involved

Minimizes time the requirement spends traversing the chain-of-command

- Upward, downward and peer-to-peer

Answers senior leadership critical questions

- Does the requirement document capture the true need?
- Is the requirement refined?
- Does the document meet the sanity check... mission oriented, what level?
- Why should we fund this... fix/broken?

RSI Big Picture

- Requirement Process currently very weak
 - Units have been very successful in getting funds with minimal disclosure
 - Currently process do not fully meet Clinger-Cohen Act, OMB or CIO accounting disciplines and mandates- RSI bolsters the effort
- Requirement Review Reports – help to focus
- Recommend an specific instruction set for requirements
 - Covers all HQ Requirements
 - Template, processes are built—confirmations on go ahead?
- Need to get the process on-line—working Enterprise Cost Management solution
- Accounting Call links investments, requirements with missions and operations

Strengthening Requirements with the RSI

- Program is vital to fix, correct, and improve deficiencies in operational mission performance— a modernization safety net
- It is critical that programs communicate it's rationale and account for expenditures with the financial and planning communities
 - The program is a continual target for fund reduction and program elimination
- Well written requirements helps all programs:
 - Articulate the need for an agency-wide Communications-Infrastructure program
 - Defend program expenditures
 - Petition for funding plus-ups

RSI Goals for the Customer

- Shows what is information is essential to HQ (A-3, FM, A-5, A-6)
 - By weighting items and using tracking features
- Provides feedback/opens dialogue to refine items
- Shows information-gaps/missing information
- Quantifies and tracks requirement progress
- Allows parent organizations to compare scores to peers'
 - Shares overall scores, not other parent organization details
- Creates universal discipline in requirement writing – goes above and beyond, fits any program
- Allows cross-functional movement of requirements between programs

RSI Goals for Program

- Shows program discipline between funds spent, technical issues and operational objectives

- Allows quantification of submitted requirements
 - Strength Indicator percentages help...
 - Seek/provide feedback to/from the customer
 - Clarify/ask for missing information
 - Validate technical issues – easier to advocate cost
 - Show rationale and accountability
 - Roll-up initiatives for wings/centers simplified

Overarching Goals of RSI

Develop a standardized accountable grading method for requirement building across the following:

- Subordinate units
- Across the agency
- Between the internal communities
- Between the organizations/agency
- Under the MAJCOM
- Across the Air Force
- Across the Departments in the DoD
- All government Agencies

The End-Goal of the RSI Is To Strengthen the Requirement Writing Process

Results of RSI

Adopting the RSI:

- Accounts for funding spent
- Breaks down cost by commodity
- Shows what funding fixed
- Shows direct correlation to mission and operations
- Provides traceability
- Baselines for budget planning

Table B-1 RSI Template

REQUIREMENT STRENGTH INDICATOR SHEET						
Program Tracking Number:					Strength Index	
Classification:						
Program TAB:					Ranking Index	
					0.00	
Ref	ITEMS	Point Value	N/A	YES	NO	Points
PART 1 - General Items						
1	Electronically Sent to Program Organizational email	15				
2	Template used	5				
3	Unit information listed	1				
4	CC Priority Provided	50				
5	A3 Priority Provided	15				
6	FM Priority Provided	10				
7	A5 Priority Provided	10				
8	A6 Priority Provided (default if not designated)	5				
9	Title	1				
10	Funding					
11	Requested Unfunded Amount (\$K)	1				
12	Partially funded by another program? remaining un-funded amount	1				
13	(for initiatives over \$250K) Is Baseline Amount listed (\$K)	1				
14	Funding type					
15	AFPOM/CCP/GDIP	1				
16	PEC or PE	1				
17	AFEE (EEIC)	1				
PART 1 - Subtotal		117				
PART 2 - Initial Description Items						
2.1 Narrative Justification			N/A	YES	NO	
1	Clear to all audiences (FM, A2, A3, A5, A6)	10				
2	Concise for presentations/databases	8				
3	Stand alone eligible (over \$250K)	5				
4	Stakeholder Information					
5	Customer/community of customers defined	1				
6	Group of end users (beneficiaries) mentioned	1				
7	Individual organization (sole recipient) mentioned	1				

8	Mission Type (Intelligence)	40				
9	Operational Names (currently supported e.g. OIF, OEF)	30				
10	Capability Needed (CN) statement included	5				
11	Service for improvement mentioned	1				
12	Process for improvement mentioned	1				
13	Products (intelligence) for improvement mentioned	1				
14	Resources needed mentioned	1				
15	Circumstances for requirement spelled out	4				
16	Mission increase (quantified/explained)	1				
17	Technology change/increase	1				
18	Funding shortfall (other program/sourcementioned)	1				
19	Deficiency of current service, process or product defined	1				
20	Quantification of need (any type) listed?	10				
21	End-state (how many or how much fixed)	10				
22	Percentage of improvement	2				
23	Quantity , number of...	10				
24	2.1 Distracting elements (n/a or yes = action not required)					
25	Is the Narrative Justification ten sentences or less					
26	Is the Narrative adequate (or is missing information severely impacting					
27	Are "total mission failure" statements supported in the submission					
28	Requirement (or phase) status updated from previous submissions					
29	Does the requirment appear similar to another submission w/o update,					
	2.2 Impact if not funded		N/A	YES	NO	
1	Quantifies mission degradation/impact					
2	Elaborates on specific mission or operational loss	20				
3	Degree of loss to mission/personnel, etc	15				
4	Potential, existing, previous violation	25				
5	Executive Order, governing body	10				
6	Law or National Policy (current state of compliance)	30				
7	Instruction (DoD, Joint, AFI, Agency)	15				
8	Downward directed initiative (circumstances stated)	10				
9	CIO or Agency corporate strategy	5				
10	Parent Organization Factors Spelled Out					
11	Parent Org CC	20				
12	Parent Org A3	15				
13	Parent Org FM	10				
14	Parent Org A5	10				
15	Parent Org A6	5				
16	Unit Organization Priority	1				

17	Parent organization POC information listed	1				
18	Subordinate Unit POC information listed	1				
19	2.2 Distracting elements (n/a or yes = action not required)					
20	Ten sentences or less as required					
21	Are "Gloom and doom type" statements quantified					
22	Shot gunned: Multiple funding sources used - explanation included					
23	Requirement items appear whole/part in another requirement					
24	Mimics other requirements (Cookie-cutter, cut and pasted)) with					
25	Same submission or phase as previous FY update is included					
	PART 2 - Subtotal	338				
	PART 3 - Supplemental Information (Detailed information)					
1	Submitter Information					
2	Parent Org Sponsor (name/rank/org)	1				
3	Unit Level Submitter (name/rank/org)	1				
4	New initiative	1				
5	Org Submittal Information					
6	Wing/Center	1				
7	Fiscal years covered (include phases)	1				
8	Type of funding (AF POM, CCP or GDIP) requested clarified	8				
9	Wing/MAJCOM approval statement	1				
	3.1 Links to Validated Planning Documents					
1	Existing Information Supporting the Requirement					
2	C4ISR Document	40				
3	Existing AF Form 3215 (include valid tracking number)	20				
4	Contract documents	15				
5	Configuration Management (CM)	20				
6	Copy of Law, Policy, etc... (from above section 2.2) included	10				
7	Professional Engineered Solutions (organizational or contract)	30				
8	Professional Cost analysis (by commodity)	30				
9	Supporting documents from outside organizations					
10	Other government Departments or Agencies	10				
11	Engineering and Installation Program	10				
12	Host nation or Host Installation agreements referenced	5				
13	Previous or related requirement referenced	12				
14	Acquisition documents	10				
15	Corporate Strategy or Enterprise Standard	10				
16	Architectural Products					
17	PWRR Submission	40				
18	Visio Products	12				

19	System Architect Product	2				
20	AutoCAD Product	5				
21	Micro Station Products	5				
22	Other CAD-type Products	5				
23	Professional/Contract Engineered Solution Products	30				
24	"As-is" baseline document included	15				
25	"To-be" future architecture document included	15				
26	Last Date Funds can be Received/Executed	1				
27	Requirement Rating (may substitute agency/org equivalent)	1				
28	Mission Critical	3				
29	Mission Impact	2				
30	Mission Essential	1				
	3.2 Expanded Justification (biggest submission impact)					
1	Mission/operation Names restated	4				
2	Identifying Reports (support documents)					
3	Inspector General (IG)	3				
4	Infrastructure Facility Assessment Team (IFAT) Reports	5				
5	Downward directed	1				
6	Miscellaneous References	1				
7	Policy Documents restated	4				
8	Other items explained	3				
9	Mission enhancements/degradations	10				
10	Alternative uses for the requirement explained	1				
11	Metrics to support the requirement	5				
12	Figures and Tables	4				
13	Additional costs (real or potential) included	5				
14	Setup	2				
15	Shipping	1				
16	Removal	2				
17	Installation	2				
18	Contract	1				
19	Restate Important Factors	1				
20	Legal Ramifications	1				
21	Loss of life, equipment, etc	5				
22	Damage or risk assessment factors	3				
23	Engineering solution cost	1				
24	De-confliction from other sources at parent organization referenced	25				
25	Partial funds from other programs or sources referenced	1				
26	Validation Statement from Parent Org	1				
27	De-conflicted with other programs via XP and FM referenced	25				

34	Resources	1				
35	Other	1				
36	Phased cost plan if requirement is over \$100K	3				
37	Waiver Memorandum (signed by Parent Org CC or DO)	10				
38	Waiver Item Commodity Breakdown (separate from approved)					
39	Software/licenses	1				
40	Telephony equipment	1				
41	Desktop Computers (PCs)	1				
42	Site analysis	1				
43	Other	1				
44	Related Project References (items not paid for by SENSOR BUS)	1				
45	Facility Mechanical and Electrical Requirement References	1				
46	Facility Space Issues/references	1				
47	Civil Engineering, etc (work order references)	1				
48	Mission type supported	1				
49	Resource Requirements	1				
50	Phases (Yes/no) supported by Phased cost plan	1				
51	Minimum funding needed	1				
52	Manpower Requirements section included and zeroed out	1				
53	Approval Official Signature block	1				
54	Part III - Distracting Elements (with relative audiences)					
	Audience					
55	Weak tie to operational mission support	A3				
56	Parts of the submission are not supported by SB	A3,A6				
57	Fund amounts exaggerated compared to similar efforts	FM				
58	No cost sources provided	FM				
59	No commodity breakdown	FM				
60	No phase breakdown (lump sum request)	FM				
61	Mixed funding type for the requirement (clarification missing)	FM				
62	Funding type not authorized for use at the unit	FM				
63	Submission not cleared through parent organization A5, FM	FM,A5				

68	No professionally engineered study/cost analysis	A6					X	
69	No CM, CSIR, AFF 3215 or host-installation documentation	A6					X	
70	Mixed network type on a single document	A6					X	
71	Architecture products missing/incomplete	A5/6					X	
72	Laws, policies, etc cited..not provided	A5/6					X	
73	Cut & paste or shot gunned requirement (w/o explanation)	A5					X	
74	Supplemental Info is weak for amount of funds requested	A5/6						
75	Minimal or no valid support documentation	A5/6						
76	For Submissions over \$250K (required if not already included)							
77	I&R Database Tracking Control Number	A3/5/6,FM						
78	Capability Needed	A3/5/6,FM						
79	Date Required	A3/5/6,FM						
80	Summary of Actions/Deliverables	A3/5/6,FM						
81	Related Projects	A3/5/6,FM						
82	Description	A3/5/6,FM						
83	Operational Objective	A3/5/6,FM						
84	Current Capability:	A3/5/6,FM						
85	Mission Impact	A3/5/6,FM						
86	Trade Off	A3/5/6,FM						
87	Facilities/Mechanical/Electrical	A3/5/6,FM						
88	Project Phases	A3/5/6,FM						
	PART 3 - Subtotal		545					

SCORING TOTAL

	available		possible	actual
Part 1 - General Items	117			
Part 2 - Initial Description Items	338			
Part 3 - Supplemental Information	545			
Total	1000			

PART I - PERCENTAGE OF DOCUMENT SCORE		
PART II - PERCENTAGE OF DOCUMENT SCORE		
PART III - PERCENTAGE OF DOCUMENT SCORE		

Parent CC Priority (x 50)		
Parent A3 Priority (x 50)		
Parent FM Priority (x 10)		
Parent A5 Priority (x 10)		
Parent A6 Priority (x 5)		
owners Priority (x 50)		
	Total	0

Comments

University of Cambridge

RSI Customer Score Sheet

Table B-2 is the score summary each parent organization receives after initial scoring of requirements. Attached to this scoring summary is a scoring sheet for each individual requirement..

Table B-2 Parent Organization Sample Summary Sheet

Tab #	Submission Number	Ranking Index	Possible Points	RSI Actual Points	RSI Percentage	\$ requested (\$K)	\$ Eligible (\$K)
A1	04296-A-xxx-003-001	7.75	765.00	60.00	7.8%	12.68	0.00
A2	04296-A-xxx-003-003	8.00	789.00	104.00	13.2%	110.91	0.00
A3	04296-A-xxx-003-006	8.25	765.00	110.00	14.4%	39.66	0.00
A4	04296-A-xxx-003-005	8.50	464.00	101.00	21.8%	5.00	0.00
A5	04296-A-xxx-003-006	8.75	767.00	143.00	18.6%	13.93	0.00
C1	04296-C-xxx-003-002	8.00	784.00	99.00	12.6%	200.89	0.00
C2	04296-C-xxx-003-004	8.25	765.00	110.00	14.4%	40.00	0.00
C3	04296-C-xxx-003-007	8.75	765.00	110.00	14.4%	70.00	0.00

Statistic Table	
Highest Score from this PO	22.5%
Average Score from this PO	16.6%
Lowest Score from this PO	7.8%
Highest Score all submissions	43.1%
Average Score all submissions	17.6%
Lowest Score all submissions	0.2%
Highest Cost PO submissions (\$K)	672.00
Average Cost PO submissions (\$K)	53.50
Lowest Cost PO submissions (\$K)	1.78
Highest Cost all submissions (\$K)	1577
Average Cost all submissions (\$K)	128
Lowest Cost all submissions (\$K)	1.78

Target Goal is 60% or higher

Target Goal is 60% or higher

Target Goal is \$100K or less per phase or submission

No target, information only

Statistic Table compares parent organizations scores against other parent organizations for informational purposes

Note: Requirement costs and details are internal to SB and not shared with other parent organizations

Submission Tracking number is created in the following manner:

- First 5 digits - Julian Date submission was received
- Letter - type of funding AF, CCP or GDIP)
- 3 digit customer number - from SB list of 150+ customers
- GIG Segment of requirement: SENSOR BUS Focus is 003
(001-Lease Lines, 002 Base infrastructure, 003 Internal building, 004-PC Refresh)
- Last 3 digits are Parent Organization SC overall priority number

INTENTIONALLY LEFT BLANK

